



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/592,916	06/13/2000	Adriano Huber	PM 258042	5750
116	7590	07/14/2006	EXAMINER	
PEARNE & GORDON LLP 1801 EAST 9TH STREET SUITE 1200 CLEVELAND, OH 44114-3108			GYORFI, THOMAS A	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 07/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/592,916

Applicant(s)

HUBER ET AL.

Examiner

Tom Gyorfi

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-37 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-37 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-37 remain for examination. The correspondence filed 4/17/06 amended claim 18 and added claims 36 and 37.

Response to Arguments

2. Applicant's arguments with respect to claims 1-37 have been considered but are moot in view of the new ground(s) of rejection.

3. In response to applicant's arguments against the references individually (see the amendment of 4/11/06: page 13, last paragraph and page 15, 2nd paragraph), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-24 and 26-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lincke (U.S. Patent 6,253,326) in view of Inoue (U.S. Patent 6,240,514), and further in view of "Wireless Authentication Protocol Wireless Transport Layer Specification" (hereinafter, "WAP WTLS").

Referring to Claim 1:

Lincke discloses a method by which a mobile subscriber with a WAP-enabled terminal can access a WEB or WAP server, comprising the steps of:

said terminal sending a request for said server to a WAP gateway (col. 8, lines 40-50), wherein encryption in the wireless interface between said WAP-enabled terminal (col. 83, lines 1-10), and

wherein an encryption protocol used by said server is based on the SSL and/or TLS security protocol (col. 111, lines 15-25); and

converting between [WTLS] and SSL and/or TLS in a secured domain of said server administrated by an administrator (col. 91, lines 50-65), wherein the [WTLS] encrypted packets sent by said terminal are routed by said gateway to said secured domain (col. 17, lines 40-50; col. 113, line 55-col. 114, line 15).

Lincke does not disclose "without said gateway decrypting all of the encrypted packets transported during a session". However, Inoue discloses a related system for a mobile wireless device to send data to a server in a manner where end-to-end encryption is realized through the use of gateways that convert the packets from one protocol with an encryption to another protocol with another encryption, without decrypting all of the encrypted data (col. 4, lines 27-32; col. 11, lines 20-37; col. 14, lines 30-42). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the functionality of Inoue into the system disclosed by Lincke. The motivation for doing so would be to eliminate potential bottlenecks in the

Art Unit: 2135

system caused by redundant decryption and re-encryption steps as found in prior art communication methods (Inoue, col. 3, lines 1-15).

Although neither Lincke nor Inoue explicitly discloses the use of WTLS, Lincke does provide for the use of alternate wireless protocols (col. 115, lines 35-40). WAP WTLS discloses the use of the WTLS protocol, which is modular and can thus be layered on top of an existing transport layer protocol, and also contains an encryption (Section 1, "Scope"; Section 5.1, "Reference Model"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use WTLS in the invention disclosed by Lincke. The motivation for doing so would be to use a technology that is widely known as an industry standard, rather than the proprietary protocol technology disclosed by Lincke, to facilitate its acceptance (WAP WTLS, Section 1, "Scope", 1st paragraph).

Referring to Claim 2:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 1 above. Lincke further discloses said gateway routes said packets to a proxy in said secured domain, said proxy using at least one protocol layer of the WAP protocol (col. 17, lines 40-45; col. 18, lines 45-68).

Referring to Claim 3:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 2 above. Lincke further discloses said packets are routed according to the URL and/or the domain name of the requested page in said gateway (col. 114, lines 20-35).

Referring to Claim 4:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 2 above. Lincke further discloses said packets are routed according to the port number (col. 114, lines 20-35).

Referring to Claim 5:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 4 above. Lincke further discloses said encrypted packets are routed according to different port numbers to different secured domains (col. 18, lines 20-35).

Referring to Claim 6:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 4 above. Lincke further discloses said port numbers are extracted in an application layer of said gateway from the URL of the request page (col. 18, lines 20-35).

Referring to Claim 7:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 6 above. Lincke further discloses said port number is extracted from only a restricted number packets during a session, and wherein the routing of at least one of the following packets depends on this extracted port number (col. 17, lines 10-25; col. 18, lines 20-40;).

Referring to Claim 8:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 7 above. Lincke further discloses wherein a proxy server in said secured domain extracts the URL and/or the port number of the received packets and where the proxy server sends back a command to said gateway if it receives a packet with a different URL and/or port number (col. 18, lines 20-68).

Referring to Claim 9:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 4 above. Lincke further discloses said port number is extracted from said URL of the required web page in said terminal (col. 18, lines 20-30).

Referring to Claim 10.

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 9 above. Lincke further discloses said port number is extracted by a browser from said URL of the required web page (col. 11, lines 15-40).

Referring to Claim 11:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 8 above. Lincke further discloses, wherein the browser in said terminal only copies said port number in said packets if an end-to-end secured connection is requested (col. 13, lines 35-50).

Referring to Claim 12:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 3 above. Lincke further discloses said packets in said gateway are routed to a secured domain if said port number is comprised in a predefined range (col. 114, lines 20-30).

Referring to Claim 13:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 3 above. Lincke further discloses said gateway sends a redirect command to said terminal if an end-to-end secured connection is requested (col. 18, lines 30-40; col. 19, lines 5-25).

Referring to Claim 14:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 13 above.

Lincke further discloses said redirect command is time limited (col. 19, lines 1-25).

Referring to Claim 15:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 13 above.

Lincke further discloses a proxy server in said secured domain extracts the URL and/or the port number of the received packets and sends a redirect command back to said terminal as soon as the session is to be routed to said gateway (col. 18, lines 35-65; col. 19, lines 1-35).

Referring to Claim 16:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 13 above.

Lincke further discloses said redirect command contains a forwarding address which is extracted from a document made accessible by said WEB or WAP server (col. 19, lines 1-20).

Referring to Claim 17:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 13 above.

Lincke further discloses said redirect command contains a document which includes the forwarding address (col. 18, lines 20-65).

Referring to Claim 18:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 13 above. Lincke [in view of WTLS] further discloses wherein said terminal sends a request for said server to said WAP gateway, wherein a browser in said terminal extracts the port number of the demanded WEB or WAP page and copies it to packets sent to said gateway (Lincke, col. 98, lines 25-34), and wherein said packets are routed, using said gateway, according to this port number (Lincke, col. 96, lines 15-30).

Referring to Claim 19:

Lincke discloses a gateway comprising:
means for receiving packets encrypted according to the [WTLS] protocol from WAP-enabled terminals (col. 18, lines 1-20, 60-68);
means for converting said packets into SSL-encrypted requests (col. 91, lines 50-51); and means for transmitting said SSL-requests to a receiving server (col. 91, lines 50-51), wherein said gateway can recognize [WTLS]-encrypted packets that are to be sent on transparently and can convert said [WTLS]-encrypted packets into SSL-encrypted request (col. 18, lines 1-65; col. 83, lines 1-20; col. 92, lines 10-15).

Lincke does not disclose “without decrypting the information contained in said [WTLS]-encrypted packets”. However, Inoue discloses a related system for a mobile wireless device to send data to a server in a manner where end-to-end encryption is realized through the use of gateways that convert the packets from one protocol with an encryption to another protocol with another encryption, without decrypting all of the

Art Unit: 2135

encrypted data (col. 4, lines 27-32; col. 11, lines 20-37; col. 14, lines 30-42). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the functionality of Inoue into the system disclosed by Lincke. The motivation for doing so would be to eliminate potential bottlenecks in the system caused by redundant decryption and re-encryption steps as found in prior art communication methods (Inoue, col. 3, lines 1-15).

Although neither Lincke nor Inoue explicitly disclose the use of WTLS, Lincke does provide for the use of alternate wireless protocols (col. 115, lines 35-40). WAP WTLS discloses the use of the WTLS protocol, which is modular and can thus be layered on top of an existing transport layer protocol, and also contains an encryption (Section 1, "Scope"; Section 5.1, "Reference Model"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use WTLS in the invention disclosed by Lincke. The motivation for doing so would be to use a technology that is widely known as an industry standard, rather than the proprietary protocol technology disclosed by Lincke, to facilitate its acceptance (WAP WTLS, Section 1, "Scope", 1st paragraph).

Referring to Claim 20:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 19 above. Lincke further discloses wherein said WTLS-encrypted packets are routed according to the URL and/or the domain name of the requested page (col. 114, lines 20-35).

Referring to Claim 21:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 19 above.

Lincke further discloses said WTLS-encrypted packets are routed according to the port number of the requested page (col. 18, lines 20-45; col. 114, lines 20-35).

Referring to Claim 22:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 21 above.

Lincke further discloses said WTLS-encrypted packets are routed to different secured domains according to different port numbers (col. 18, lines 20-45).

Referring to Claim 23:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 21 above.

Lincke further discloses said port number is extracted from the URL of the requested page in an application layer of said gateway (col. 8, lines 5-35).

Referring to Claim 24:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claim 21 above.

Lincke further discloses said port number is extracted during a session only from a restricted number of WTLS-encrypted packets,
and wherein the routing of at least one following WTLS-encrypted packet depends on said extracted port number (col. 17, lines 10-30; col. 18, lines 20-40).

Referring to Claims 26 and 31:

A method for performing end-to-end secure data transfer between a terminal and a server, wherein said terminal is connected to said server via a wireless connection between said terminal and a gateway, said method comprising the steps of:

said terminal requesting a secure communication session with said server via said gateway, said requesting including the steps of (col. 17, lines 40-50):

said terminal generating a request including request packets encrypted using a [WTLS] protocol (col. 83, lines 1-20), said terminal sending said request to said gateway, said gateway forwarding said request to said server or to another server (col. 18, lines 20-45), wherein said gateway does not decrypt all of said request packets, and said server or said another server decrypting some number of said request packets using said [WTLS] protocol (col. 91, lines 50-60); and

said server or said another server serving data to said terminal via said gateway, said serving including the steps of:

said server or said another server sending said data including data packets encrypted using said [WTLS] protocol to said gateway (col. 114, line 45-col. 115, line10);

said gateway forwarding said data packets to said terminal (col. 18, lines 20-35); and said terminal decrypting said data packets using said WTLS protocol (col. 89, lines 5-20).

Lincke does not disclose "wherein said gateway does not decrypt all of said data packets". However, Inoue discloses a related system for a mobile wireless device to

Art Unit: 2135

send data to a server in a manner where end-to-end encryption is realized through the use of gateways that convert the packets from one protocol with an encryption to another protocol with another encryption, without decrypting all of the encrypted data (col. 4, lines 27-32; col. 11, lines 20-37; col. 14, lines 30-42). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the functionality of Inoue into the system disclosed by Lincke. The motivation for doing so would be to eliminate potential bottlenecks in the system caused by redundant decryption and re-encryption steps as found in prior art communication methods (Inoue, col. 3, lines 1-15).

Although Lincke does not explicitly disclose the use of WTLS, it does provide for the use of alternate wireless protocols (col. 115, lines 35-40). WAP WTLS discloses the use of the WTLS protocol, which is modular and can thus be layered on top of an existing transport layer protocol, and also contains an encryption (Section 1, "Scope"; Section 5.1, "Reference Model"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use WTLS in the invention disclosed by Lincke. The motivation for doing so would be to use a technology that is widely known as an industry standard, rather than the proprietary protocol technology disclosed by Lincke, to facilitate its acceptance (WAP WTLS, Section 1, "Scope", 1st paragraph).

Referring to Claims 27 and 32:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claims 26 and 31 above. Lincke further discloses said gateway must decrypt some but not all of said

request packets to forward said request to said server or said another server (col. 18, lines 20-35).

Referring to Claims 28 and 33:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claims 27 and 32 above. Lincke further discloses said gateway must decrypt some but not all of said data packets to forward said data to said terminal (col. 18, lines 45-60).

Referring to Claims 29 and 34:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claims 26 and 32 above. Lincke further discloses a browser on said terminal provides information to said gateway for forwarding said request to said server or said another server without said gateway decrypting any of said request packets (col. 11, lines 25-50).

Referring to Claims 30 and 35:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claims 29 and 34 above. Lincke further discloses said information includes one or more of: a port number, a domain name, and an URL (col. 18, lines 20-45).

Referring to Claims 36 and 37:

Lincke, Inoue, and WAP WTLS disclose the limitations of Claims 1 and 19 above. Lincke further discloses wherein said gateway determines whether an end-to-end

Art Unit: 2135

secured routing is requested according to the URL of the requested page (col. 35, lines 29-37; col. 83, lines 1-10).

6. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lincke in view of Inoue.

Referring to Claim 25:

Lincke discloses a method by which a terminal can access a server, said method comprising the steps of:

said terminal sending a request for said server to a gateway, wherein security utilized between said terminal and said gateway is based on a first security protocol, said first security protocol including an encryption (col. 83, lines 59-67);

securing said server with a second security protocol, said second security protocol also including an encryption (col. 83, lines 1-10; col. 91, lines 50-60);

converting between said first and second security protocol in a secured domain of said server administrated by a administrator or in said gateway (col. 91, lines 50-60).

Lincke does not disclose wherein "encrypted packets sent by said terminal are routed by said gateway to said secured domain without said gateway decrypting all of the packets during a session." However, Inoue discloses a related system for a mobile wireless device to send data to a server in a manner where end-to-end encryption is realized through the use of gateways that convert the packets from one protocol with an encryption to another protocol with another encryption, without decrypting all of the

Art Unit: 2135

encrypted data (col. 4, lines 27-32; col. 11, lines 20-37; col. 14, lines 30-42). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the functionality of Inoue into the system disclosed by Lincke. The motivation for doing so would be to eliminate potential bottlenecks in the system caused by redundant decryption and re-encryption steps as found in prior art communication methods (Inoue, col. 3, lines 1-15).

Conclusion

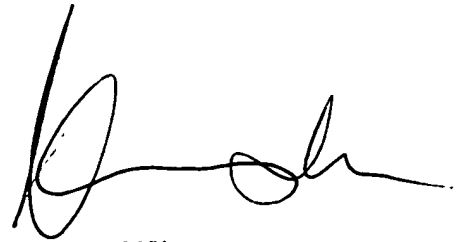
7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: U.S. Patents 6,523,068; 6,480,717; and 6,266,704.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
7/6/06

A handwritten signature in black ink, appearing to read 'Kim Vu', with a stylized, flowing script.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100